FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1435988-0

Total Deleted Page(s) = 2
Page 15 ~ b6; b7C; b7E;
Page 16 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

b6
b7C

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/22/2011

To: Norfolk

From: Norfolk
Squad 10
Contact: SA [redacted]

b3
b6
b7C
b7E

Approved By: [redacted] KR

Drafted By: [redacted] djd

Case ID #: (U) [redacted]

(U) **Title:** (U) SUSPICIOUS ACTIVITY THAT RELATES TO GLOBAL STRATEGIES GROUP (NORTH AMERICA) INC.; [redacted]

Synopsis: (U) To close case.

~~**Derived From :** FBI NSISCG-20080301~~
~~**Classified By:** J12387T63~~
~~**Declassify On:** 20360822~~

Details: (U) In December 2010, SA [redacted] conducted research into the two links provided in the suspicious email: http://news.bbc.co.uk/2/hi/middle_east/2988455.stm and http://www.jonathanforeman.com/military/nyp_iraq/04192003_chest.html. Research identified that both links go to legitimate sites documenting the discovery of a "$700 Million Treasure Chest" by the U.S. military in Iraq and that both links have been used for years in connection with known spam emails.

b6
b7C

(U) Since December 2010, FBI Norfolk has not received any other complaints from this victim concerning suspicious emails. With the conclusion of all investigative research into this suspicious email and the lack of a nexus to spear phishing, malicious code, [redacted] it is recommended that this case be closed.

b3
b7E

◆◆

CLOSE CASE
CY
8/22/2011
KR
DONE 8/23/11

~~SECRET//NOFORN~~

b3
b7E

b6
b7C

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/14/2011

To: Norfolk

From: Norfolk
Squad 10
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] djd

Case ID #: (U) [redacted]

b3
b6
b7C
b7E

(U) **Title:** (U) SUSPICIOUS ACTIVITY THAT RELATES TO GLOBAL STRATEGIES GROUP (NORTH AMERICA) INC.; [redacted]

Synopsis: (U) To document continued research conducted on suspicious email.

~~**Derived From:** FBI NSISCG-20080301~~
~~**Declassify On:** 20351215~~

Details: (U) On 12/13/2010, SA [redacted] received an email from [redacted] for Global Strategies Group (North America) Inc. also known as Global Defense Technology & Systems, Inc. (GTEC) regarding a new suspicious email received by a GTEC employee, [redacted] on 12/11/2010. This email appears to have been sent from lieutenant [redacted] All of the text in the email is contained in the subject line, which reads: "I am [redacted] an officer of the U.S Army. I am on the move to Afghanistan from Iraq as the last batch just left and have some items I will need to ship to you. Can you be trusted?" This email was marked as spam by the [redacted] email account. [redacted] informed [redacted] that the email contained one blocked image that contains the actual message, which is at https://img.web.de/v/p.gif. Neither [redacted] accessed this message.

b6
b7C

(U) [redacted] included the email header information which upon review identified the originating Internet Protocol (IP)

b6
b7C

To: Norfolk From: Norfolk
Re: (U) [redacted] (Pending), 01/14/2011 b3 b7E

address: 41.138.164.40. [redacted] identified that this IP belongs to Visafone Communications Limited based in Lagos, Nigeria.

(U) A review of ACS for [redacted] b6 b7C b7E As such, no further investigative action will be taken at this time.

(U) A copy of the email from [redacted] and the printouts from [redacted] have been placed in a 1-A envelope and made part of this case file.

♦♦

b6
b7C

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 12/14/2010

To: Norfolk

From: Norfolk
Squad 10
Contact: SA [redacted]

Approved By: [redacted] KL

Drafted By: [redacted] djd

b3
b6
b7C
b7E

Case ID #: (U) [redacted]
(U)

Title: (U) ~~(S)~~ SUSPICIOUS ACTIVITY THAT RELATES TO GLOBAL STRATEGIES GROUP (NORTH AMERICA) INC.; [redacted]

Synopsis: (U) To document continued research conducted on suspicious email.

~~**Derived From :** FBI NSISCG-20080301~~
~~**Declassify On:** 20351214~~

Details: (U) On 12/14/2010, SA [redacted] received an email from [redacted] for Global Strategies Group (North America) Inc. also known as Global Defense Technology & Systems, Inc. (GTEC) containing the header information for the suspicious email received by a GTEC employee on 11/16/2010. This email appears to have been sent from [redacted] explained that the GTEC employee that received the email, [redacted] received it at his old work email account, [redacted] is not familiar with the [redacted] account. SFA is the former name of GTEC, and all of their old email accounts are still active.

b6
b7C

(U) A review of the email header information identified 59.185.102.44 as the originating Internet Protocol (IP) address for this email. Multiple IP look ups identified that this IP belongs to Mahanagar Telephone Nigam Ltd (MTNL-AP), located in Mumbai, India.

~~SECRET//NOFORN~~

To: Norfolk From: Norfolk
Re: (U) [redacted] (Pending), 12/14/2010

b3
b7E

(U) A review of Automated Case Support (ACS) for [redacted]

b7E

[redacted]

(U) [redacted]

b7E

(U) ACS and internet research for [redacted]

b6
b7C
b7E

(U) Administrative: a copy of the IP look up from [redacted] has been placed in a 1-A envelope and made part of this case file.

♦♦

b6
b7C

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 12/13/2010

To: Norfolk

From: Norfolk
Squad 10
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

b3
b6
b7C
b7E

Case ID #: (U) [redacted]
(U)

(U) **Title:** (~~S~~) SUSPICIOUS ACTIVITY THAT RELATES TO GLOBAL STRATEGIES GROUP (NORTH AMERICA) INC.; [redacted]

Synopsis: (U) To document research conducted on suspicious email.

~~**Derived From :** FBI NSISCG-20080301~~
~~**Declassify On:** 20351213~~

Details: (U) On 12/13/2010, SA [redacted] searched Automated Case Support (ACS), and conducted google searches regarding [redacted]

b6
b7C
b7E

(U) (~~S~~//~~NF~~) ACS research into [redacted]

b7E

~~SECRET//NOFORN~~

b3
b7E

[redacted]

To: Norfolk From: Norfolk b3
Re: (U) [redacted] (Pending), 12/13/2010 b7E

[redacted] b7E

(U) [redacted]

[redacted] b7E

(U) An ACS search for [redacted]

[redacted] b7E

(U) On 12/13/2010, SA [redacted] emailed [redacted] the [redacted] for Global Strategies Group (North America) Inc. also known as Global Defense Technology & Systems, Inc. (GTEC) and requested email header information regarding this suspicious email. b6 b7C

♦♦

b6
b7C

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/24/2010

To: Norfolk

From: Norfolk
Squad 10
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] djd

b3
b6
b7C
b7E

Case ID #: (U) [redacted]

(U) **Title:** (~~S~~) SUSPICIOUS ACTIVITY THAT RELATES TO GLOBAL STRATEGIES GROUP (NORTH AMERICA) INC.; [redacted]

Synopsis: (U) To document research into suspicious email and contact with victim company

~~**Derived From:** FBI NSISCG-20080301~~
~~**Declassify On:** 20351124~~

Details: (U) On 11/23/2010, SA [redacted] queried [redacted] in Automated Case Support (ACS). [redacted]

b6
b7C
b7E

(U) On 11/24/2010, SA [redacted] contacted [redacted] the [redacted] for Global Strategies Group (North America) Inc. also known as Global Defense Technology & Systems, Inc. (GTEC) at office telephone [redacted]

b6
b7C

(U) [redacted] noted that GTEC has not received any other similar emails and nothing further has come from this incident. [redacted] also read part of the Defense Security Service investigative report on this matter, which identified that this email was analyzed and does not appear to be connected with any intelligence collection activities. [redacted] volunteered to forward any additional suspicious emails to SA [redacted] for the duration of this case.

b6
b7C

◆◆

~~SECRET//NOFORN~~

b3
b7E

[redacted]

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/21/2010

To: Norfolk **Attn:** Squad 10

From: Norfolk
Squad 10
Contact: SA

Approved By:

Drafted By: djd

(U) **Case ID #:** ~~(S)~~

(U) **Title:** ~~(S)~~ SUSPICIOUS ACTIVITY THAT RELATES TO GLOBAL STRATEGIES GROUP (NORTH AMERICA) INC.;

Synopsis: (U) To open a Full Investigation.

~~**Derived From :** FBI NSISCG 20080301~~
~~**Declassify On:** 20351004~~

Details: (U) On 08/31/2010, with Defense Security Service (DSS) notified FBI Norfolk via email of a suspicious contact report concerning Global Strategies Group (North America) Inc. also known as Global Defense Technology & Systems, Inc. (GTEC). GTEC is located at 760 Lynnhaven Parkway, Suite 200, Virginia Beach, VA 23452.

(U) received an email on 08/23/2010, from with office telephone and email: for GTEC. This email identified that an employee with GTEC, received an email stating that someone whom works with left office keys at the bar. The email included a link which the sender stated contained a picture of the found keys. Neither nor anyone else at GTEC clicked on the link.

(U) The original email, dated 8/20/2010 at 11:18PM, appears to come from [mailto: The link included in the email is: http://www.ionplatform.com/cgi-bin/arp3/arp3-t.pl?l=140&c=1904402.

(U) Due to the above information, it is requested that this case be opened and assigned to SA

CM SA
CPI Code None
Source Code 07
Date/Initials 10/21/10 DDT

Full

◆◆

~~SECRET//NOFORN~~

101004- GTEC Opening

1A1

b3
b6
b7C
b7E

FD-340 (Rev. 4-11-03)

File Number [redacted]

Field Office Acquiring Evidence PH

Serial # of Originating Document [redacted]

Date Received 12/13/10

From [redacted]
(Name of Contributor/Interviewee)

760 Lynnhaven Parkway Suite 200
(Address)

b6
b7C

Virginia Beach, VA
(City and State)

By SA [redacted]

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: Suspicious Activity Report related to Global Strategies Group (North America) INC.;
[redacted]

Reference: _____
(Communication Enclosing Material)

b3
b6
b7C
b7E

Description: ☐ Original notes re interview of

Email from [redacted] re emirates

KR

[redacted]

From: [redacted]
Sent: Monday, December 13, 2010 8:53 AM
To: [redacted] b6 b7C
Subject: FW: Suspicious Email 12/13/2010

[redacted]

Below, at the very bottom is a suspicious email forwarded to me from one of my employees working remote from his home [redacted]
There are a couple of email exchanges here, as you'll see, because the entire email is contained in the subject line. This concerned me, so I emailed him back to check if there were any blocked items or attachments that came with the email. He responded back with an image link that had been blocked. I went ahead and had him send me the expanded headers to save time if it turns out this is something that needs further investigation. I have included them below. Please let me know if you need any additional information.

Microsoft Mail Internet Headers Version 2.0
Received: from gnavbmx1.gna.local ([172.16.2.55]) by [redacted] with Microsoft SMTPSVC(6.0.3790.4675);
Sat, 11 Dec 2010 13:42:56 -0500
Received: from smtp1.gtec-inc.com (172.16.4.2) by gnamcmx1.gna.local
(172.16.2.55) with Microsoft SMTP Server id 8.1.436.0; Sat, 11 Dec 2010
13:42:56 -0500
X-ASG-Debug-ID: 1292092975-66a5f64d0001-edubRe
Received: from fmmailgate09.web.de (fmmailgate09.web.de [217.72.192.184]) by
[redacted]
[redacted]
[redacted] b6 b7C b7E
From: [redacted]
To: [redacted]
Message-ID: <328736392.1319406.1292092971771.JavaMail.fmail@mwmweb004>
Subject: [SPAM] I am [redacted] an officer of the U.S Army. I am on the move to Afghanistan from Iraq as the last batch just left and have some items I will need to ship to you. Can you be trusted?
MIME-Version: 1.0
X-ASG-Orig-Subj: I am [redacted] an officer of the U.S Army. I am on the move to
Afghanistan from Iraq as the last batch just left and have some items I
will need to ship to you. Can you be trusted?
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 7bit
Sensitivity: Normal
X-Provags-ID: V01U2FsdGVkX1/sY1zy1xXSfOejehGVF0bDq1bLj7pZCml0vd7PLT3P7aOs9lZAccb/
Rkcw8YK++VmoPzYeWs33Eg==
X-Barracuda-Connect: fmmailgate09.web.de[217.72.192.184]
X-Barracuda-Start-Time: 1292092975
X-Barracuda-URL: http://172.16.4.2:8000/cgi-mod/mark.cgi
X-Virus-Scanned: by bsmtpd at gtec-inc.com
X-Barracuda-Bayes: INNOCENT GLOBAL 0.4827 1.0000 0.0000
X-Barracuda-Spam-Score: 1.05
X-Barracuda-Spam-Status: No, SCORE=1.05 using global scores of TAG_LEVEL=1.6 QUARANTINE_LEVEL=2.2 KILL_LEVEL=2.6
tests=HTML_MESSAGE, HTML_MIME_NO_HTML_TAG, MIME_HTML_ONLY
X-Barracuda-Spam-Report: Code version 3.2, rules version 3.2.2.49140
Rule breakdown below
pts rule name description
---- ---------- ----------
0.00 MIME_HTML_ONLY BODY: Message only has text/html MIME parts
0.00 HTML_MESSAGE BODY: HTML included in message
1.05 HTML_MIME_NO_HTML_TAG HTML-only message, but there is no HTML tag
X-Priority: 5 (Lowest)

X-MSMail-Priority: Low
Importance: Low
X-Barracuda-Spam-Flag: YES
Return-Path: col47@irgmll.co.cc
X-OriginalArrivalTime: 11 Dec 2010 18:42:56.0818 (UTC) FILETIME=[3A3E8920:01CB9963]

Source:

<body bgcolor="#ffffff" background="https://img.web.de/v/p.gif" class="bgRepeatYes" style="background-repeat: repeat; background-color: rgb(255, 255, 255); color: rgb(0, 0, 0); font-family: verdana,geneva; font-size: 9pt; padding-left: 0px;">   </body>

[redacted]

o: [redacted]
f:
e:
w: www.gtec-inc.com

b6
b7C

From: [redacted]
Sent: Monday, December 13, 2010 7:47 AM
To: [redacted]
Subject: RE: [SPAM] I am [redacted] an officer of the U.S Army. I am on the move to Afghanistan from Iraq as the last batch just left and have some items I will need to ship to you. Can you be trusted?

No, not if it requires opening the link. I will forward this along with your previous email to DSS.

Thanks,

[redacted]

o: [redacted]
f:
e:
w: www.gtec-inc.com

b6
b7C

From: [redacted]
Sent: Monday, December 13, 2010 7:45 AM
To: [redacted]
Subject: RE: [SPAM] I am [redacted] an officer of the U.S Army. I am on the move to Afghanistan from Iraq as the last batch just left and have some items I will need to ship to you. Can you be trusted?

It's got blocked images that I assume are the email. I'm not exactly sure what I'm doing, but I think this is the link that contains the actual message: https://img.web.de/v/p.gif

Do you want me to pull down the message and forward it to you?

From: [redacted]
Sent: Monday, December 13, 2010 7:41 AM
To: [redacted]
Subject: RE: [SPAM] I am [redacted] an officer of the U.S Army. I am on the move to Afghanistan from Iraq as the last batch just left and have some items I will need to ship to you. Can you be trusted?

b6
b7C

This is the entire email? No links or anything?

[redacted]

o: [redacted]
f:
e:
w: www.gtec-inc.com

From: [redacted]
Sent: Monday, December 13, 2010 7:26 AM
To: [redacted]
Subject: FW: [SPAM] I am [redacted] an officer of the U.S Army. I am on the move to Afghanistan from Iraq as the last batch just left and have some items I will need to ship to you. Can you be trusted?
Importance: Low

b6
b7C

[redacted]

Global Strategies Group (North America) Inc.

o: [redacted]
e:
w: www.gtec-inc.com

A Global Defense Technology & Systems Company (NASDAQ: GTEC)

Mission-Critical Solutions for National Security

From: lieutenant [redacted]
Sent: Saturday, December 11, 2010 1:43 PM
To: [redacted]
Subject: [SPAM] I am [redacted] an officer of the U.S Army. I am on the move to Afghanistan from Iraq as the last batch just left and have some items I will need to ship to you. Can you be trusted?
Importance: Low

b6
b7C